Trójkąt Stirlinga dla cykli:

$$
\begin{array}{ccccccccccc}
 & & & & \begin{bmatrix}0\\0\end{bmatrix} & & & & & & \\
 & & & \begin{bmatrix}1\\0\end{bmatrix} & & \begin{bmatrix}1\\1\end{bmatrix} & & & & & \\
 & & \begin{bmatrix}2\\0\end{bmatrix} & & \begin{bmatrix}2\\1\end{bmatrix} & & \begin{bmatrix}2\\2\end{bmatrix} & & & & \\
 & \begin{bmatrix}3\\0\end{bmatrix} & & \begin{bmatrix}3\\1\end{bmatrix} & & \begin{bmatrix}3\\2\end{bmatrix} & & \begin{bmatrix}3\\3\end{bmatrix} & & & \\
\begin{bmatrix}4\\0\end{bmatrix} & & \begin{bmatrix}4\\1\end{bmatrix} & & \begin{bmatrix}4\\2\end{bmatrix} & & \begin{bmatrix}4\\3\end{bmatrix} & & \begin{bmatrix}4\\4\end{bmatrix} & & \\
\begin{bmatrix}5\\0\end{bmatrix} & & \begin{bmatrix}5\\1\end{bmatrix} & & \begin{bmatrix}5\\2\end{bmatrix} & & \begin{bmatrix}5\\3\end{bmatrix} & & \begin{bmatrix}5\\4\end{bmatrix} & & \begin{bmatrix}5\\5\end{bmatrix} \\
 & & & & \vdots & & & & & &
\end{array}
$$

Trójkąt Stirlinga dla cykli:

$$
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 0 & & 1 & & & & & \\
 & & 0 & & 1 & & 1 & & & & \\
 & 0 & & 2 & & 3 & & 1 & & & \\
0 & & 6 & & 11 & & 6 & & 1 & & \\
 & 24 & & 50 & & 35 & & 10 & & 1 & \\
 & & & & \vdots & & & & & &
\end{array}
$$

Twierdzenie

Wzór

$$x^{\overline{n}} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k$$

zachodzi dla każdej liczby całkowitej dodatniej n.

- Zauważmy, że jak w powyższym wzorze podstawimy $x = 1$, to otrzymamy jeden z omawianych wcześniej wzorów.
- Dowód powyższego twierdzenia można przeprowadzić indukcyjnie — podobnie do przeprowadzonego wcześniej dowodu analogicznego twierdzenia dla liczb Stirlinga drugiego rodzaju (należy pamiętać, że $x^{\overline{n}} = (x + n - 1)x^{\overline{n-1}}$).

Trójkąt Stirlinga dla podzbiorów:

$$
\begin{array}{ccccccccccccccccc}
 & & & & & & \left\{ {0 \atop 0} \right\} & & & & & & & & & & \\
 & & & & \left\{ {1 \atop 0} \right\} & & & & \left\{ {1 \atop 1} \right\} & & & & & & & & \\
 & & & \left\{ {2 \atop 0} \right\} & & & \left\{ {2 \atop 1} \right\} & & & & \left\{ {2 \atop 2} \right\} & & & & & & \\
 & & \left\{ {3 \atop 0} \right\} & & & \left\{ {3 \atop 1} \right\} & & & \left\{ {3 \atop 2} \right\} & & & & \left\{ {3 \atop 3} \right\} & & & & \\
 & \left\{ {4 \atop 0} \right\} & & & \left\{ {4 \atop 1} \right\} & & & \left\{ {4 \atop 2} \right\} & & & \left\{ {4 \atop 3} \right\} & & & & \left\{ {4 \atop 4} \right\} & & \\
\left\{ {5 \atop 0} \right\} & & \left\{ {5 \atop 1} \right\} & & & \left\{ {5 \atop 2} \right\} & & & \left\{ {5 \atop 3} \right\} & & & \left\{ {5 \atop 4} \right\} & & & \left\{ {5 \atop 5} \right\} \\
 & & & & & & \vdots & & & & & & & & &
\end{array}
$$

Trójkąt Stirlinga dla podzbiorów:

$$
\begin{array}{ccccccccccccccccc}
 & & & & & & 1 & & & & & & & & & & \\
 & & & & & 0 & & 1 & & & & & & & & & \\
 & & & & 0 & & 1 & & 1 & & & & & & & & \\
 & & & 0 & & 1 & & 3 & & 1 & & & & & & & \\
 & & 0 & & 1 & & 7 & & 6 & & 1 & & & & & & \\
 & 0 & & 1 & & 15 & & 25 & & 10 & & 1 & & & & & \\
 & & & & & & \vdots & & & & & & & & & &
\end{array}
$$

Twierdzenie

Dla $n > 0$ zachodzi zależność rekurencyjna

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}.$$

Poniższy dowód jest modyfikacją wcześniej przedstawionego dowodu zależności rekurencyjnej dla liczb Stirlinga drugiego rodzaju.

Dowód. *(1/2)*

Niech $S = \{a_1, a_2, \ldots, a_n\}$. Określimy liczbę podziałów S na k cykli $C_1, C_2, \ldots, C_k$. Zauważmy, że w każdym takim podziale elementy $a_1, a_2, \ldots, a_{n-1}$ można rozmieścić albo w cyklach $C_1, C_2, \ldots, C_{k-1}$ albo w cyklach $C_1, C_2, \ldots, C_{k-1}, C_k$.

W pierwszym przypadku mamy $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ możliwości. Zayważmy, że dla każdego takiego podziału element a_n tworzy ostatni, jednoelementowy cykl $C_k = [a_n]$.

- $\binom{n}{k}$ — liczba k-elementowych podzbiorów zbioru n-elementowego
- $\left\{ {n \atop k} \right\}$ — liczba podziałów n-elementowego zbioru na k niepustych podzbiorów
- $\left[{n \atop k} \right]$ — liczba permutacji n-elementowego zbioru zawierających k cykli

Liczby Stirlinga pierwszego rodzaju nazywane są *liczbami cyklicznymi Stirlinga*, a drugiego rodzaju — *liczbami podzbiorowymi Stirlinga*.

Wartości $\begin{bmatrix} n \\ k \end{bmatrix}$ dla małych wartości k:

- $k = 0$.

  Podobnie jak w przypadku liczb Stirlinga drugiego rodzaju mamy $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$ oraz $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ dla $n > 0$.

- $k = 1$.

  Oczywiście $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$. Pamiętamy, że zbiór n-elementowy ma dokładnie $n!$ permutacji. Każdemu cyklowi odpowiada dokładnie n permutacji (każda rozpoczyna się od innego elementu danego zbioru), zatem

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{n!}{n} = (n-1)!$$

Liczby Stirlinga drugiego rodzaju

Definicja

Podziałem skończonego zbioru S nazywamy rodzinę parami rozłącznych podzbiorów $\{S_1, S_2, \ldots, S_k\}$ zbioru S taką, że

$$S_1 \cup S_2 \cup \ldots \cup S_k = S.$$

Definicja (liczby Stirlinga drugiego rodzaju)

Symbol $\left\{ {n \atop k} \right\}$ (czyt. k podzbiorów n) oznacza liczbę sposobów podziału zbioru n-elementowego na k niepustych podzbiorów.

Liczby Stirlinga drugiego rodzaju występują częściej niż liczby Stirlinga pierwszego rodzaju, więc zaczynamy od nich — tak jak James Stirling w swojej książce *Methodus Differentialis* (1730).

Dowód. *(2/2)*

W drugim przypadku mamy $\left\{ {n-1 \atop k} \right\}$ możliwości podziału zbioru $\{a_1, a_2, \ldots, a_{k-1}\}$ na $S_1, S_2, \ldots, S_k$. Zauważmy, że w przypadku każdego takiego podziału element a_n może trafić do jednego z k zbiorów $S_1, S_2, \ldots, S_k$. Zatem w tym przypadku mamy $k \cdot \left\{ {n-1 \atop k} \right\}$ możliwości.

Ostatecznie

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}.$$

□

Wartości $\left\{ {n \atop k} \right\}$ dla małych n i k:

n \ k	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0
7	0	1	63	301	350	140	21	1	0	0
8	0	1	127	966	1701	1050	266	28	1	0
9	0	1	255	3025	7770	6951	2646	462	36	1

Uwaga!

W przypadku, gdy $n \geqslant 0$ i $k < 0$ zakładamy, że $\left\{ {n \atop k} \right\} = 0$.

Wartości $\left\{ {n \atop k} \right\}$ dla małych wartości k:

- $k = 0$.
  Przyjmujemy, że $\left\{ {0 \atop 0} \right\} = 1$. Jeżeli $n > 0$ to, oczywiście, $\left\{ {n \atop 0} \right\} = 0$.
- $k = 1$.
  Mamy $\left\{ {0 \atop 1} \right\} = 0$. Dla $n > 0$ istnieje dokładnie jeden n-elementowy podział n-elementowego zbioru, więc
  $$\left\{ {n \atop 1} \right\} = 1.$$
- $k = 2$.
  Oczywiście $\left\{ {0 \atop 2} \right\} = 0$. Załóżmy, że $n > 0$. Chcemy rozbić zbiór $S = \{a_1, a_2, \ldots, a_n\}$ na dwa podzbiory S_1 i S_2. Bez straty ogólności możemy przyjąć, że $a_1 \in S_1$. Pozostałe a_i możemy przypisać do zbioru S_1 na 2^{n-1} sposobów, ale musimy pamiętać, że nie możemy do niego przypisać wszystkich elementów zbioru S. Zatem
  $$\left\{ {n \atop 2} \right\} = 2^{n-1} - 1.$$

Odwrotny algorytm Euklidesa

Algorytm służy wyznaczenia u i v takich, że $a \cdot u + b \cdot v = \text{NWD}(a, b)$.

- Obliczamy $\text{NWD}(a, b)$ korzystając z algorytmu Euklidesa otrzymując ciąg równań
  $a = q_1 \cdot b + r_1, \quad b = q_2 \cdot r_1 + r_2, \quad r_1 = q_3 \cdot r_2 + r_3, \quad \ldots,$
  $r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}, \quad r_{n-2} = q_n \cdot r_{n-1} + r_n, \quad r_{n-1} = q_{n+1} \cdot r_n.$
- Z i-tego równania wyznaczamy wartość r_i dla każdego $i = 1, 2, \ldots, n$ (więc pomijamy ostatnie równanie).
- Wyliczone r_n daje nam równanie
  $\text{NWD}(a, b) = r_{n-2} - q_n \cdot r_{n-1}$.
  Do tego równania wstawiamy wyliczoną wartość r_{n-1} (w ten sposób otrzymujemy $\text{NWD}(a, b)$ w kombinacji liniowej r_{n-2} i r_{n-3}).
- Kontynuujemy podstawianie r_{n-2}, r_{n-3} itd. aż do r_1, po drodze upraszczając współczynniki. W efekcie dostajemy zapis implikujący wartości u i v.

Słowniczek

$\lvert x\rvert$	wartość bezwzględna liczby x
NWD(a, b)	największy wspólny dzielnik liczb a i b
NWW(a, b)	najmniejsza wspólna wielokrotność liczb a i b
$\min\{a, b\}$	niewiększa z liczb a i b
$\max\{a, b\}$	niemniejsza z liczb a i b
$a \mid b$	liczba a jest dzielnikiem liczby b
$a \perp b$	liczby a i b są względnie pierwsze
$\mathbb{N}$	zbiór liczb naturalnych, $\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z}$	zbiór liczb całkowitych, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}_n$	zbiór reszt z dzielenia przez n, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
$\mathbb{P}$	zbiór liczb pierwszych
p_i	i-ta liczba pierwsza

Definicja

Liczba $n \in \mathbb{N}$ jest **liczbą pierwszą**, jeżeli n ma dokładnie dwa dodatnie dzielniki.

- 0 nie jest liczbą pierwszą (po pierwsze nie jest liczbą dodatnią, a po drugie ma nieskończenie wiele dzielników).
- 1 nie jest liczbą pierwszą (ma dokładnie jeden dodatni dzielnik).
- Początkowe liczby pierwsze: $2, 3, 5, 7, 11, 13, 17, 19, 23$.
- Liczby naturalne większe od 1 dzielimy na liczby pierwsze i liczby złożone (złożone to te, które nie są pierwsze).
- 1 nie jest ani liczbą pierwszą, ani liczbą złożoną.
- Zbiór liczb pierwszych oznaczamy przez $\mathbb{P}$.

Definicja NWW

Niech $a, b \in \mathbb{Z}/\{0\}$. Liczbę $D \in \mathbb{N}$ nazywamy **najmniejszą wspólną wielokrotnością** liczb a i b, gdy

- $a|D$ i $b|D$,
- jeżeli dla $c \in \mathbb{N}$ mamy $a|c$ i $b|c$, to $D|c$.

Najmniejszą wspólną wielokrotność liczb a i b oznaczamy jako NWW(a, b).

Przykład

NWW$(6, 8) = 24$, NWW$(14, -17) = 238$, NWW$(-3, -9) = 9$.

W literaturze często można spotkać się z oznaczeniami NWD$(a, b) = (a, b)$ i NWW$(a, b) = [a, b]$.

Definicja NWD

Niech $a, b \in \mathbb{Z}$ i niech co najmniej jedna z nich jest różna od 0. Liczbę naturalną d nazywamy **największym wspólnym dzielnikiem** liczb a i b, gdy

- $d|a$ i $d|b$,
- jeżeli dla $c \in \mathbb{N}$ mamy $c|a$ i $c|b$, to $c|d$.

Największy wspólny dzielnik liczb a i b oznaczamy jako $\mathrm{NWD}(a, b)$.

Przykład

$\mathrm{NWD}(6, 8) = 2, \quad \mathrm{NWD}(14, -17) = 1, \quad \mathrm{NWD}(-3, -9) = 3, \quad \mathrm{NWD}(0, 24) = 24.$

Przykład

Wyznaczyć największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność liczb 48 i 180.
Stosując algorytm Euklidesa otrzymujemy

$$\begin{aligned} 180 &= 3 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 \end{aligned}$$

Zatem $\mathrm{NWD}(48, 180) = 12$.

Z faktu $\mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b) = |a \cdot b|$ otrzymujemy $\mathrm{NWW}(a, b) = \dfrac{|a \cdot b|}{\mathrm{NWD}(a, b)}$.

Zatem

$$NWW(48, 180) = \frac{48 \cdot 180}{12} = \frac{4 \cdot 180}{1} = 720.$$

Czy z powyższego dowodu wynika, że liczba P jest liczbą pierwszą? Nie!

$$
\begin{aligned}
2+1 &= 3 \in \mathbb{P}\\
2\cdot 3+1 &= 7 \in \mathbb{P}\\
2\cdot 3\cdot 5+1 &= 31 \in \mathbb{P}\\
2\cdot 3\cdot 5\cdot 7+1 &= 211 \in \mathbb{P}\\
2\cdot 3\cdot 5\cdot 7\cdot 11+1 &= 2311 \in \mathbb{P}\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1 &= 59\cdot 509\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17+1 &= 19\cdot 97\cdot 277\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19+1 &= 347\cdot 27\,953\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23+1 &= 317\cdot 703\,763\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29+1 &= 331\cdot 571\cdot 34\,231\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31+1 &= 200\,560\,490\,131 \in \mathbb{P}\\
2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37+1 &= 181\cdot 60\,611\cdot 676\,421
\end{aligned}
$$

Zatem konstrukcja w powyższym dowodzie nie daje przepisu na tworzenie coraz większych liczb pierwszych, a jedynie wskazuje, że istnieją liczby pierwsze nienależące do dowolnego skończonego zbioru liczb pierwszych.

Stwierdzenie

Dla dowolnej liczby pierwszej p i liczby całkowitej dodatniej α zachodzi:

- $\varphi(p) = p - 1$,
- $\varphi(p^\alpha) = p^\alpha \cdot \left(1 - \frac{1}{p}\right)$.

Dowód.

- Liczba pierwsza p jest względnie pierwsza z każdą z liczb $1, 2, \ldots, p-1$.
- Zauważmy, że jedynie wielokrotności liczby pierwszej p mają wspólny nietrywialny dzielnik z p^α. Zatem w zbiorze $\{1, 2, \ldots, p^\alpha - 1\}$ liczbami niebędącymi liczbami względnie pierwszymi z p^α są

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{\alpha-1} - 1) \cdot p,$$

więc ich liczba wynosi $p^{\alpha-1} - 1$. Zatem

$$\varphi\left(p^\alpha\right) = \left(p^\alpha - 1\right) - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

□

Definicja

Dla każdej liczby $n \in \mathbb{N}/\{1\}$ określamy liczbę $\varphi(n)$ jako liczbę dodatnich liczb całkowitych mniejszych od n i względnie pierwszych z n:

$$\varphi(n) = \Big|\{1 \leqslant k < n : \ k \perp n\}\Big|.$$

Funkcję $\varphi = \varphi(n)$ nazywamy **funkcją φ-Eulera**.

Przykład

Obliczmy NWD$(k, 12)$ dla k mniejszych od 12:

$$\begin{array}{llll} \text{NWD}(1,12) = 1, & \text{NWD}(4,12) = 4, & \text{NWD}(7,12) = 1, & \text{NWD}(10,12) = 2, \\ \text{NWD}(2,12) = 2, & \text{NWD}(5,12) = 1, & \text{NWD}(8,12) = 4, & \text{NWD}(11,12) = 1. \\ \text{NWD}(3,12) = 3, & \text{NWD}(6,12) = 6, & \text{NWD}(9,12) = 3, & \end{array}$$

Zatem

$$\varphi(12) = \Big|\{1,5,7,11\}\Big| = 4.$$

Twierdzenie

Liczb pierwszych jest nieskończenie wiele.

Dowód.

Załóżmy nie wprost, że teza twierdzenia jest fałszywa, tj. zbiór liczb pierwszych jest skończony. Zatem dla pewnej liczby naturalnej n mamy

$$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}.$$

Niech P będzie następnikiem iloczynu wszystkich elementów powyższego zbioru $\mathbb{P}$:

$$P = 1 + \prod_{i=1}^{n} p_i.$$

Zauważmy, że liczba P przy dzieleniu przez p_i (dla $i = 1, 2, \ldots, n$) daje resztę 1, zatem liczba P nie jest podzielna przez żadną liczbę pierwszą — uzyskaliśmy sprzeczność. □

Powyższy dowód ma ∼2500 lat (*Elementy* Euklidesa).